SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY:	EXECUTIVE ORDER 10450, 9397, AND PUBLIC LAW 99-474, THE COMPUTER FRAUD AND ABUSE ACT
PURPOSE OF USE:	TO RECORD NAMES, SIGNATURES, AND SOCIAL SECURITY NUMBERS FOR THE PURPOSE OF VALIDATING THE TRUSTWORTHINESS OF INDIVIDUALS REQUESTING ACCESS TO DEPARTMENT OF DEFENSE (DOD) SYSTEMS AND INFORMATION.
ROUTINE USES:	THOSE GENERALLY PERMITTED UNDER THE 5 U.S.C. 522A(B) OF THE PRIVACY ACT AS REQUIRED.
DISCLOSURE:	DISCLOSURE OF THIS INFORMATION IS VOLUNTARY; HOWEVER, FAILURE TO PROVIDE THE REQUESTED INFORMATION MAY IMPEDE, DELAY OR PREVENT FURTHER PROCESSING OF THIS REQUEST.
NOTE:	RECORDS MAY BE MAINTAINED IN BOTH ELECTRONIC AND/OR PAPER FORM.

TYPE OF REQUEST
□ INITIAL □ MODIFICATION □ DELETION □ USER ID ____________

DATE

SYSTEM NAME *(Platform or Applications)*

LOCATION *(Physical Location of System)*

PART I: *(To be completed by Requestor)*

1. NAME *(LAST, FIRST, MI)*

2. SOCIAL SECURITY NUMBER

3. ORGANIZATION

4. OFFICE SYMBOL/DEPARTMENT

5. PHONE *(DSN or Commercial)*

6. OFFICIAL E-MAIL ADDRESS

7. JOB TITLE & GRADE/RANK

8. OFFICIAL MAILING ADDRESS

USER AGREEMENT (COMPLETE BLOCK 29 OR 30 AS APPROPRIATE)

I accept the responsibility for the information and DOD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DISA/DOD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

9. USER SIGNATURE

10. DATE

PART II: SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OF CLEARANCE INFORMATION.

11. CLEARANCE LEVEL

11a. ADP DESIGNATION

12. TYPE OF INVESTIGATION

12a. DATE

13. VERIFIED BY: *(Print name)*

14. SIGNATURE

15. DATE

PART III: ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number and date of contract expiration in Block 16).*

16. JUSTIFICATION FOR ACCESS

17. TYPE OF ACCESS REQUIRED: □ AUTHORIZED □ PRIVILEGED

18. USER REQUIRES ACCESS TO: □ UNCLASSIFIED □ CLASSIFIED *(Specify Category)*
□ OTHER ____________

19. VERIFICATION OF NEED TO KNOW
I certify that this user requires access as requested. □

19a. EXPIRATION DATE FOR ACCESS *(Specify date if less than 1 year)*

20. SUPERVISOR'S NAME *(Print name)*

21. SUPERVISOR'S SIGNATURE

22. DATE

23. SUPERVISOR'S ORGANIZATION/DEPARTMENT

23a. PHONE NUMBER

24. SIGNATURE OF FUNCTIONAL DATA OWNER/OPR

24a. PHONE NUMBER

24b. DATE

25. SIGNATURE OF ISSO

26 ORG./DEPARTMENT

27. PHONE NUMBER

28. DATE

29. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS: *(Complete as required for user or functional level access)*

□ I HAVE COMPLETED DOD INFORMATION AWARENESS CD. DATE ____________

30. SYSTEM ADMINISTRATOR/DISA SSP CERTIFICATION LEVEL:

□ LEVEL I ______________________________

□ LEVEL II *(Indicate Operating System(s))* ______________________________

□ LEVEL III ______________________________

31. OPTIONAL INFORMATION

PART IV: COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED	PROCESS BY: *(Print name and sign)*	DATE
DATE REVALIDATED	REVALIDATE BY: *(Print name and sign)*	DATE

INSTRUCTIONS

A. Part I: The following information is provided by the user when establishing or modifying their USERID.

(1) Name: The last name, first name, and middle initial of the user
(2) Social Security Number: The social security number of user.
(3) Organization: The user's current DISA organization (i.e. DISA CIO, DOD and government agency or commercial firm)
(4) Office Symbol/Department: The office symbol within the current organization (i.e. CIO/IAD)
(5) Telephone Number/DSN: The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
(6) Official Email Address: The user's official email address.
(7) Job Title/Grade/Rank: The job title civilian (EX. Systems Analyst, GS-14, Pay Clerk, GS-5)/, military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.
(8) Official Mailing Address: The user's official mailing address
(9) User's Signature: User must sign the DISA Form 41 with the understanding that they are responsible and accountable for their password and access to the system(s).
(10) Date: The date that the user signs the form.

B. Part II. Certification of Background Investigation or Clearance.

(11) Clearance Level: The user's current security clearance level (Secret, Top Secret).
(11a) ADP Designation: The user's ADP Designation (ADP1, ADP3, etc).
(12) Type of Investigation. The user's last type of background investigation. (i.e., NAC, NACI, or SSBI)
(12a) Date : Date of last investigation.
(13) Verified By: The Security Manager or his representative print his/her name that the above clearance and investigation information has been verified
(14) Signature: The Security Manager or his representative signature indicates that the above clearance and investigation information has been verified.
(15) Date: The date that the form was signed by the Security Manager or his representative.

C. Part III. The below information requires the endorsement from the User's Supervisor or the Government Sponsor.

(16) Justification for Access: A brief statement is required to justify establishment of an initial USERID. Provide appropriate information if the USERID or access to the current USERID is to modified.
(17) Type of Access Required: Place an "X" in the appropriate box. (Authorized- Individual with normal access) (Privileged- Those with privilege to amend or change system configuration, parameters, or settings)
(18) User Requires Access to: Place an "X" in the appropriate box. Specify Category.
(19) Verification of Need to Know: To verify that the user requires access as requested.
(19a) Expiration Date for Access: The user must specify expiration date if less than 1 year.
(20) Supervisor's Signature (Print Name): The supervisor or representative prints his/her name that the above information has been verified and access is required.
(21) Supervisor's Signature: Supervisor's signature is required by the endorser or his/her representative.
(22) Supervisor Date: Date he/she signs the form.
(23) Supervisor's Organization/Department: Supervisor's organization and department
(23a) Supervisor's Phone Number: Supervisor's phone number
(24) Signature of Functional Data Owner/OPR: Signature of the functional appointee responsible for approving access to the system being requested.
(24a) Phone Number: Functional appointee phone number
(24b) Date: The date the Functional appointee signs the DISA Form 41
(25) Signature of ISSO: Signature of the ISSO or sponsoring office responsible for approving access to the system being requested.
(26) ORG./Dept: ISSO's organization and department
(27) Phone Number: ISSO's Phone number
(28) Date: The date ISSO signed the SAAR Form.
(29) IA Training and Awareness Certification Requirements: User must indicate if they have completed the DOD Information Awareness CD and the date
(30) System Administrator/DISA SSP Certification Level: Place an "X" in the appropriate certification level box.
(31) Optional Use: This section is intended to add site specific information, as required.

D. Part IV. This information is site specific and can be customized by either the DECC, functional activity, or the customer with approval of the DECC. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DECC or by the Customer's ISSO. Recommend file be maintained by ISSO adding the user to the system.